

*The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.*

**TLP: WHITE**

**Traffic Light Protocol (TLP): WHITE information may be distributed without restriction, subject to copyright controls.**

<http://www.us-cert.gov/tlp/>

**DATE(S) ISSUED:**

10/13/2016

**SUBJECT:**

Multiple Vulnerabilities in Google Chrome Could Allow for Remote Code Execution

**OVERVIEW:**

Multiple vulnerabilities have been discovered in Google Chrome, the most severe of which could result in remote code execution. Google Chrome is a web browser used to access the Internet. These vulnerabilities can be exploited if a user visits, or is redirected to, a specially crafted web page. Successful exploitation of these vulnerabilities could allow an attacker to execute remote code in the context of the browser, obtain sensitive information, bypass security restrictions, or cause denial-of-service conditions.

**THREAT INTELLIGENCE:**

There are currently no reports of these vulnerabilities being exploited in the wild.

**SYSTEM AFFECTED:**

- Google Chrome prior to 54.0.2840.59

**RISK:**

**Government:**

- Large and medium government entities: **High**
- Small government entities: **Medium**

**Businesses:**

- Large and medium business entities: **High**
- Small business entities: **Medium**

**Home users: Low**

**TECHNICAL SUMMARY:**

Multiple vulnerabilities have been discovered in Google Chrome, the most severe of which could result in remote code execution. These vulnerabilities can be exploited if a user visits, or is redirected to, a specially crafted web page. Details of the vulnerabilities are as follows:

- Universal XSS in Blink and Bookmarks (CVE-2016-5181)
- Heap Overflow in Blink (CVE-2016-5182)
- Use after free in PDFium (CVE-2016-5183, CVE-2016-5184)
- Use after free in Blink. (CVE-2016-5185)

- URL Spoofing. (CVE-2016-5187, CVE-2016-5189)
- UI Spoofing. (CVE-2016-5188)
- Cross-origin Bypass in Blink (CVE-2016-5192)
- Out of Bounds read in DevTools. (CVE-2016-5186)
- Universal XSS in Bookmarks (CVE-2016-5191)
- Use after free in Internals (CVE-2016-5190)
- Scheme Bypass (CVE-2016-5193)
- Various fixes from internal audits, fuzzing and other initiatives (CVE-2016-5194)

Successful exploitation of these vulnerabilities could allow an attacker to execute remote code in the context of the browser, obtain sensitive information, bypass security restrictions, or cause denial-of-service conditions.

#### **RECOMMENDATIONS:**

The following actions should be taken:

- Apply appropriate patches provided by Google to vulnerable systems immediately after appropriate testing.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.
- Inform and educate users regarding the threats posed by hypertext links contained in emails or attachments especially from un-trusted sources.

#### **REFERENCES:**

##### **Google:**

<https://googlechromereleases.blogspot.com/2016/10/stable-channel-update-for-desktop.html>

##### **CVE:**

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-5181>  
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-5182>  
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-5183>  
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-5184>  
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-5185>  
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-5186>  
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-5187>  
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-5188>  
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-5189>  
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-5190>  
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-5191>  
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-5192>  
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-5193>  
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-5194>

**Traffic Light Protocol (TLP): WHITE information may be distributed without restriction, subject to copyright controls.**

**<http://www.us-cert.gov/tlp/>**